From the discussion held regarding the initial scan of the website, it appeared that others experienced similar outcomes. This exercise has simulated an initial penetration test on a target website. From this, we have found potential vulnerabilities that can be exploited, such as the lack of MX record can cause reputational damage to a website (Fraud Watch, 2016).

It appeared that Traceroute (Linux) or tracert (Windows) provided a similar number of hops for teams scanning different websites; however, they also experienced similar issues regarding the timeouts. For example, we found a difference in hop count when using TCP route and ICMP traceroute. TCP provided less hops and a more realistic route, whereas ICMP showed more hops but an unrealistic route. This is because, generally, ICMP can be flagged as low priority traffic. ICMP packets have lower priority than TCP packets and are therefore not always sent on the shortest way along their route. (Parziale et al., 2006)

It also seems that many other teams are using similar tools, such as Tracert, NMap, and MTR to conduct the security scans of the websites. This is expected as the tools used are standard tools for penetration testing and scanning. All provide the basic information required to start exploiting vulnerabilities, but they should never be used solely in isolation.

The information identified by the scans, can be used to exploit further. For example, using ping provides the IP Address and confirmation that the server is responding to a ping command. Nmap can be used to identify potential target devices on the network. This can then be used further to monitor those identified hosts for other activities (Ferranti, M., 2018).To add to the initial scans conducted, further scanning will be planned using the tools mentioned in the discussion. This will be done following a step-by-step process in line with penetration testing standards.

References

Fraud Watch (2016) Email Security: MX Records. Available from: [**https://fraudwatchinternational.com/phishing/email-security-mx-records/**](https://fraudwatchinternational.com/phishing/email-security-mx-records/) [Accessed 5 June 2021]

Ferranti, M (2018) What is Nmap? Why you need this network mapper. Available from:

<https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html> [Accessed 10 June]

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) *TCP/IP Tutorial And Technical Overview.* 8th ed. New York: IBM.